AUDIT OF COMPUTER APPLICATIONS

Our audit of computer applications is based on the GAO guidelines, ***Assessing the Reliability of Computer-Processed Data***. According to these guidelines:

When computer-processed data are an important or integral part of the audit and the data's reliability is crucial to accomplishing the audit objectives, auditors need to satisfy themselves that the data are relevant and reliable. This is important regardless of whether the data are provided to the auditor or the auditor independently extracts them. To determine the reliability of the data, the auditors may either (a) conduct a review of the general and application controls in the computer-based systems including tests as are warranted; or (b) if the general and application controls are not reviewed or are determined to be unreliable, conduct other tests and procedures.

When the reliability of a computer-based system is the primary objective of the audit, the auditor should conduct a review of the system's general and application controls.

"General Controls" refer to the structure, methods, and procedures that apply to the overall computer operations in an agency. They include organization and management controls, security controls, and system software and hardware controls.

"Application Controls" refer to the methods and procedures designed for each application to ensure the authority of data origination, the accuracy of data input, integrity of processing, and verification and distribution of output.

AUDIT PROGRAM

A. PRELIMINARY SURVEY

The EDP Auditor will follow the regular City Auditor procedures for the Preliminary Survey.

B. RISK ASSESSMENT

The EDP Auditor will follow the regular City Auditor procedures for Risk Assessment.

C. AUDIT PROCEDURES

(NOTE: The EDP auditor may reduce or expand these procedures depending upon the results of the Preliminary Survey and Risk Assessment.)

REVIEW OF GENERAL CONTROLS

1. Determine whether the computer system meets the needs of the City.

1.a Determine whether objectives and policies for the computer application have been put in writing and approved by senior management.

1.b Determine whether the system features and the related objectives met by each feature have been documented.

1.c Determine whether Application Performance Measures (APMs) have been identified and an APM strategy is in place (See page 6).

2. Determine whether important activities and functions in maintaining the computer systems are performed.

2.a Determine whether the department has a process for documenting general and application control procedures.

2.b Determine whether the department has provided adequate training and supervision to all personnel responsible for performing control procedures.

2.c Determine whether the department has prepared written statements of responsibilities to assign responsibility for specific activities and functions. Survey staff to ascertain that these statements of responsibilities are current.

2.d Determine whether the department has prepared a written maintenance schedule.

2.e Determine whether supervisory reviews are performed and documented to ascertain that specific activities and functions are performed as scheduled.

3. Determine whether the department has procedures in place to ensure that the computer system is able to recover after a disaster or computer failure.

3.a Determine whether the department has a backup and recovery plan and a schedule for periodic testing of the plan.

3.b Determine whether the department uses offsite storage for backup files.

3.c Determine whether the department has conducted tests to reconstruct systems and databases from data held in off-site storage. Review the documentation of the test results.

4. Determine whether the department has procedures to ascertain that no unauthorized changes in the computer systems are made.

4.a Determine whether the department requires that appropriate written authorization be obtained before a system change is initiated. Determine whether all changes are supported by a standard request form that describes the nature of and reason for the system change.

4.b Determine whether the department has implemented software and physical measures to prevent and detect unauthorized changes to systems software and applications.

5. Determine whether the department has procedures to ensure that information processing problems are timely detected and corrected.

5.a Determine whether the department maintains a record of all problems and the follow-up actions taken. Ascertain that the maintenance record is current and complete.

5.b Determine whether the department maintains a record of manufacturers' warranties and ascertains that all repairs that are within the warranty period are performed under the warranty.

6. Determine whether the department has procedures and controls to secure and properly care for its computer equipment.

6.a Determine whether the department maintains an inventory of computer equipment, including computer units, terminals, printers, and input devices.

6.b Determine whether the department has affixed permanent City labels on all its computer equipment.

6.c Determine whether the department has assigned responsibility for each piece of computer equipment to a specific employee.

6.d Determine whether the department performs an annual physical inventory of computer equipment and prepares a written report of the inventory, including an investigation of any lost or damaged equipment.

7. Determine whether the department has procedures or controls to ensure that unauthorized individuals do not tamper with sensitive data and program files.

7.a Determine whether the department has provided an appropriate level of security for sensitive data files and programs.

7.b Determine whether the department has established and enforced standards to control the use of passwords.

7.c Determine whether the department utilizes appropriate physical and logical access controls to secure the IT application's supervisory and utility programs.

7.d Determine whether the department employees lock computer terminals and other computer equipment or keep them in secure areas.

7.e When information systems processing is carried out at multiple sites with extensive use of telecommunications, determine whether the department uses specific and appropriate telecommunications security techniques.

7.f Determine whether the department has written policies and procedures to ascertain that software licenses are valid and no pirated software is being used.

REVIEW OF APPLICATION CONTROLS

8. Determine whether the department has procedures to ensure that only authorized, correct, and complete transactions are processed.

8.a Determine whether the department has written procedures to ensure that only authorized and correct transactions are processed.

8.b Determine whether the department uses sequentially numbered transactions and investigates the reasons for missing numbers. If the department does not use sequential numbering, find out what other strategy the department follows to ensure complete processing.

8.c Determine what types of input checks are incorporated in the system and whether these input checks are sufficient to ensure that no unauthorized, erroneous, or incomplete transactions are processed.

9. Determine whether the department has procedures to ensure that authorized transactions are processed timely, completely, and accurately.

9.a Determine whether the department has established and enforced standards to ensure timely, complete, and accurate processing of authorized transactions.

9.b Determine whether the department uses control totals to check the completeness of processing. If the department does not use control totals, find out what other strategy the department follows to ensure complete processing.

9.c Determine whether staff performs and documents independent reviews to ascertain that number sequence integrity and control totals are effectively used to check the completeness of processing.

9.d Determine whether the department files its transaction records in a planned sequence to facilitate retrieval.

10. Determine whether the department has procedures or controls to ensure that the IT application's output is complete, accurate, and consistent.

10.a Determine whether the IT application provides software capability to scrutinize and analyze data.

10.b Determine whether the department has incorporated control totals in report summaries. If the department does not use control totals, find out what other strategy the department follows to ensure the completeness and accuracy of computer reports.

10.c Determine whether the department requires independent staff to compare summary records to the supporting detailed records and check the consistency of multiple versions of data, as well as report consistency from period to period.

APM STRATEGY

According to the Governmental Accounting Standards Board, a governmental entity ideally should:

- **establish and communicate clear and relevant goals and objectives**
- **set measurable targets for accomplishment, and**
- **develop and report indicators that measure its progress in achieving those goals and objectives.**

Application Performance Measures (APM) are the indicators that measure an IT application's progress in achieving its goals and objectives.

In designing an APM Strategy for its IT applications, the department should:

1. Define the IT application's goals and objectives. Clearly defined goals and objectives are key to an effective APM process.
2. Define baseline requirements and means of measuring performance. You cannot implement an APM process without establishing meaningful measurements and comparison points.
3. Establish a system of rewards and penalties. Without such a system, the staff responsible for the IT application have no incentive to achieve the application goals and objectives.
4. Implement tools to monitor the APM process. Unless you monitor performance, you have no way of knowing if the IT Application is meeting its purpose.